Defense Information System Network (DISN)
Video Services Web Site
Security Guide

February 2008
Version 1.0

Defense Information Systems Agency
DISN Video Services Division (GS25)
P.O. Box 4502
Arlington, Virginia 22204-4502

Table of Contents

1.0 Purpose/Scope

In this User Access Security Guide we will review the new Public Key Infrastructure (PKI) security requirements and provide guidance for installing Department of Defense (DoD) Root Certificates and accessing the protected area of the DISN Video Services (DVS) Web site using a PKI smart card.

Effective 6:30 PM EST, Thursday, 28 February 2008, the DVS Web site (DVS-WS) will be PK-Enabled to require client based certificate authentication. On implementation, the cryptographic log-on process will require the use of a Common Access Card (CAC) and embedded PKI certificates to authenticate a user's identification. Contractors or other individuals not eligible for DoD PKI certificates must obtain a valid External Certification Authority (ECA) PKI certificate, or HSPD-12 cards by non-DoD federal agencies. Detailed information on PKI policy and PKI certificates follows. Note: After CAC login, DVS Users will still use their current DVS-WS User ID and Password to access the DVS-WS application.

2.0 Introduction

Authentication is crucial to secure communications. Users must be able to prove their identity to those with whom they communicate and must be able to verify the identity of others. Authentication of identity on a network is complex because the communicating parties do not physically meet as they communicate. This can allow an unethical person to intercept messages or to impersonate another person or entity. A method must be worked out to maintain the necessary level of trust within the communication process.

To meet this requirement, Secure Socket Layer (SSL) is currently in use on DVS-WS servers. The SSL protocol allows applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. SSL provides endpoint authentication and communications privacy over the Internet using cryptography. Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (whether an individual or an application, such as a Web browser) can be sure with whom they are communicating.

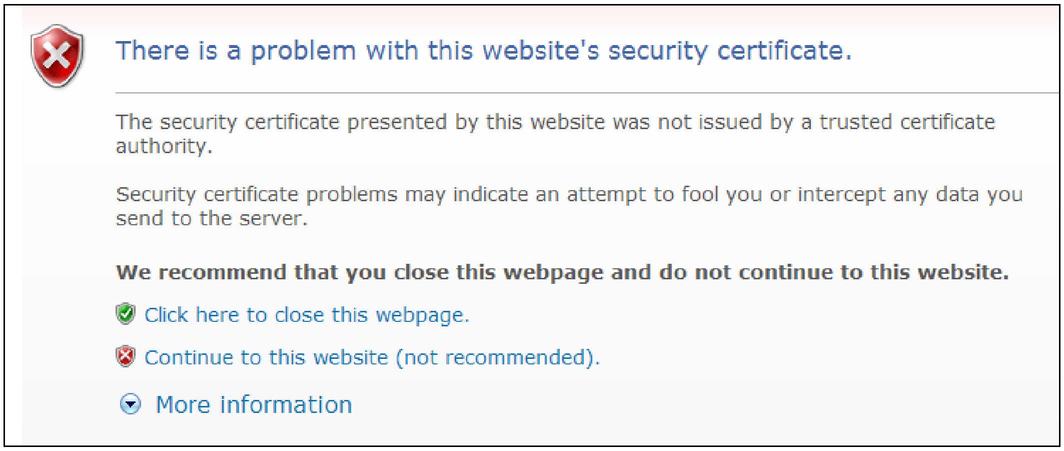
The next level of security—when both ends of the "conversation" are sure with whom they are communicating—is known as mutual authentication. Mutual authentication requires public key infrastructure (PKI) deployment to clients. PKI is mandated by DoD Directive (DoDD) 8190.3, "Smart Card Technology", 31 August 2002, and JTF-GNO Communications Tasking Order (CTO) 06-02 Accelerated PKI Implementation. DVS Customers will be required use either a DoD CAC, ECA, or HSPD-12 card to access DVS-WS. In some cases, ECA certificate software can replace the use of a physical card.

3.0 Installing DoD Root Certificates

Using certificates for authentication depends on having certificates issued by a trusted certificate issuer. Certificates for trusted certificate issuers are typically kept in the ROOT store of your browser. Installing the DoD Root Certificates will allow *your* Web browser to trust the identity of Web sites, such as DVS-WS, whose secure communications are authenticated by the DoD.

Is this required?
No, however, this will help you avoid Security Alert windows when you to go to secure communication web sites for various DoD agencies.

Shown below are Security Certificate Warning messages that are displayed when the DoD Root Certificate is *not* installed.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

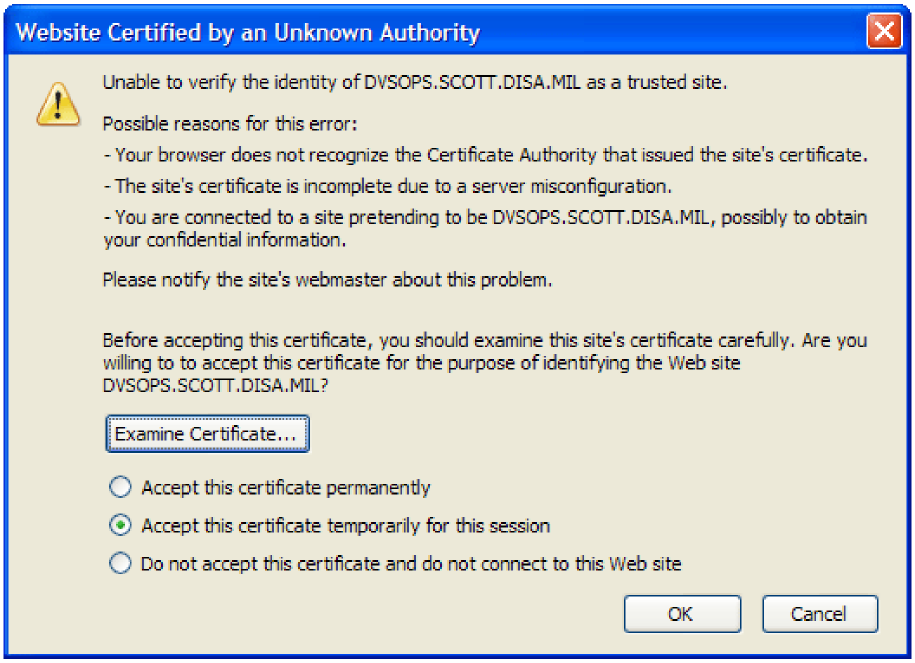
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure 1. Security Certificate Warning in Internet Explorer



Website Certified by an Unknown Authority

Unable to verify the identity of DVSOPS.SCOTT.DISA.MIL as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be DVSOPS.SCOTT.DISA.MIL, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site DVSOPS.SCOTT.DISA.MIL?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site

Figure 2. Security Certificate Warning in Netscape Navigator

IMPORTANT: You <u>must</u> use the DVS-WS domain name (https://dvsops.scott.disa.mil) to test if the certificates are installed. If you use the IP address (https://209.22.91.136), you will receive the certificate-warning message even if the certificates are installed properly.

Avoiding these certificate-warning messages (above) is easy to correct by installing the DoD Root CA certificates in your browser. There are three certificates that should be installed:

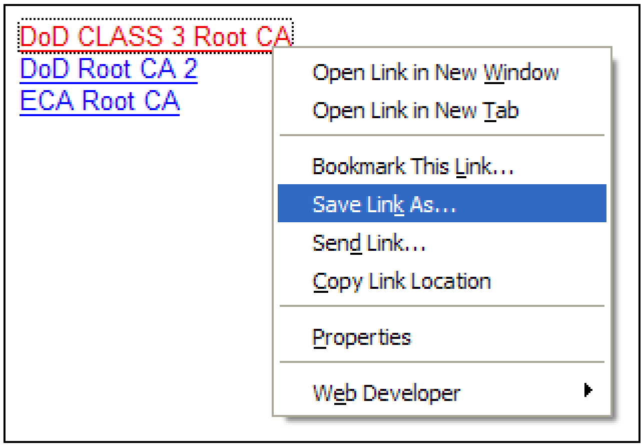
- DoD CLASS 3 Root CA
- DoD Root CA 2
- ECA Root CA

4.0 Download DoD Root Certificate Authority (CA) Certificates

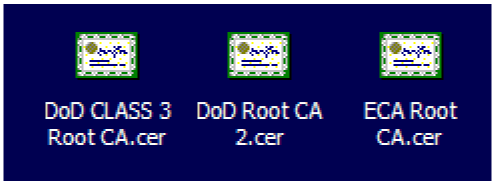
The DoD Root Certificates are available for download from the DVS Public web site.

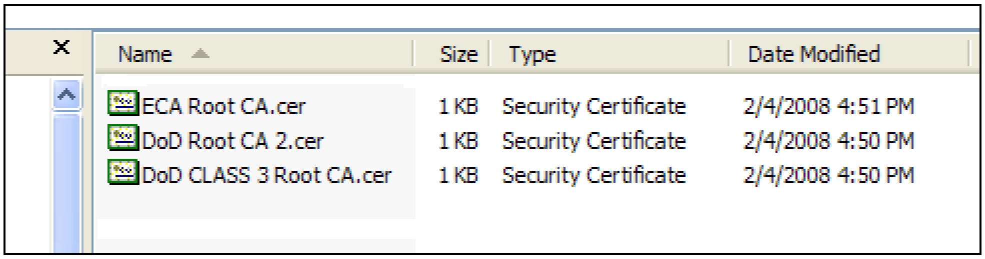
1. Navigate to URL address: http://www.disa.mil/disnvtc/pki.htm

2. Right click each certificate and select, “Save Link As.” Save the files to your Desktop (recommended) or local directory of your choice.



The certificate files will appear on the Desktop or local directory.

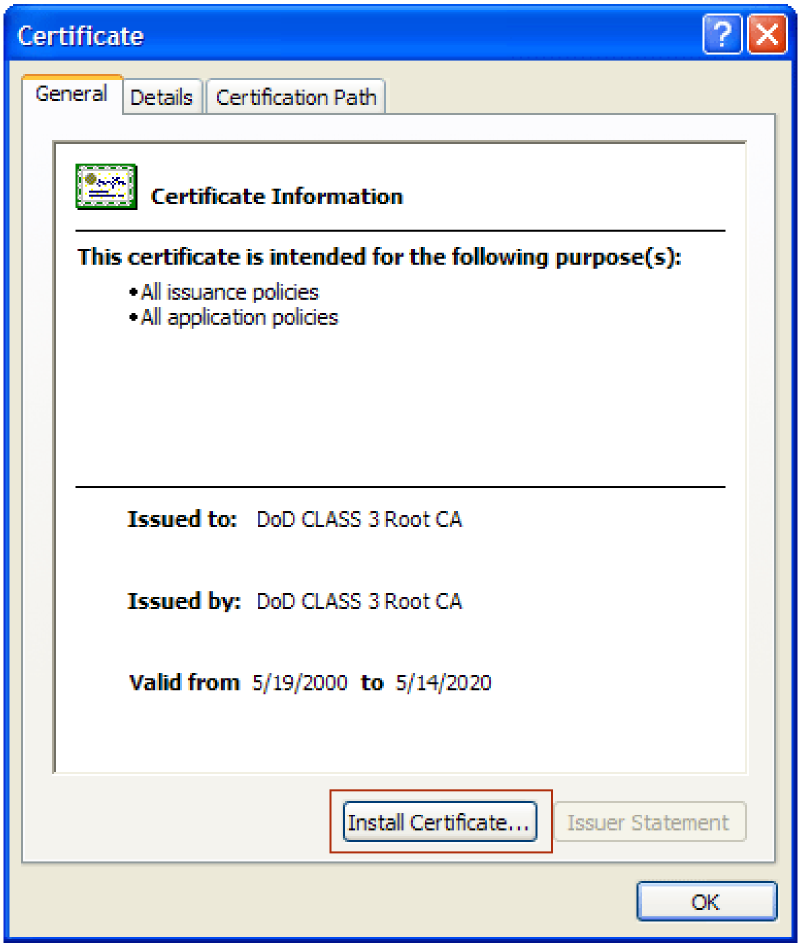




Name	Size	Type	Date Modified
ECA Root CA.cer	1 KB	Security Certificate	2/4/2008 4:51 PM
DoD Root CA 2.cer	1 KB	Security Certificate	2/4/2008 4:50 PM
DoD CLASS 3 Root CA.cer	1 KB	Security Certificate	2/4/2008 4:50 PM

5.0 Install DoD Root CA Certificates in Internet Explorer (IE)

1. Double-click on the "DoD CLASS 3 Root CA.cer" file. The Certificate window displays. Click the Install Certificate button. Note that installing the certificates is done through Windows (not IE). IE will automatically find the certificate store.



Certificate Information

This certificate is intended for the following purpose(s):

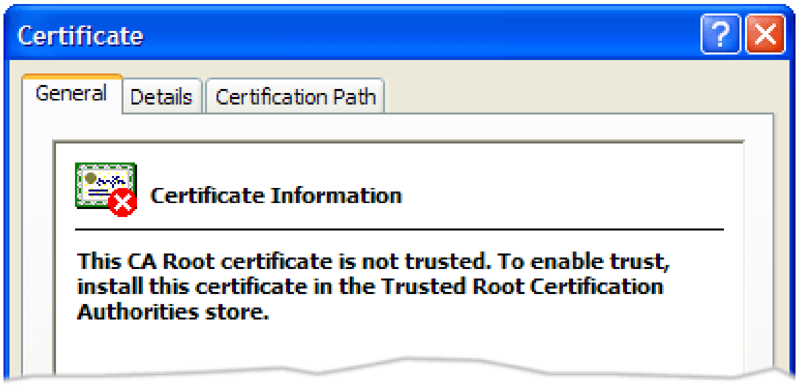
- All issuance policies
- All application policies

Issued to: DoD CLASS 3 Root CA

Issued by: DoD CLASS 3 Root CA

Valid from 5/19/2000 to 5/14/2020

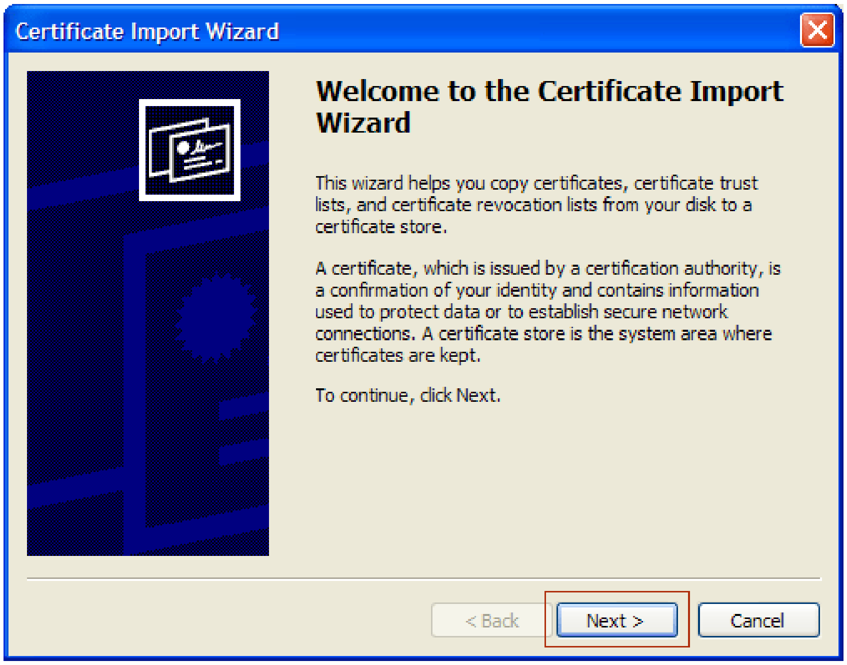
Note: You may receive a warning message that this CA Root certificate is not trusted. This is normal. You can continue with the installation.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

2. Click the Next button.



Certificate Import Wizard

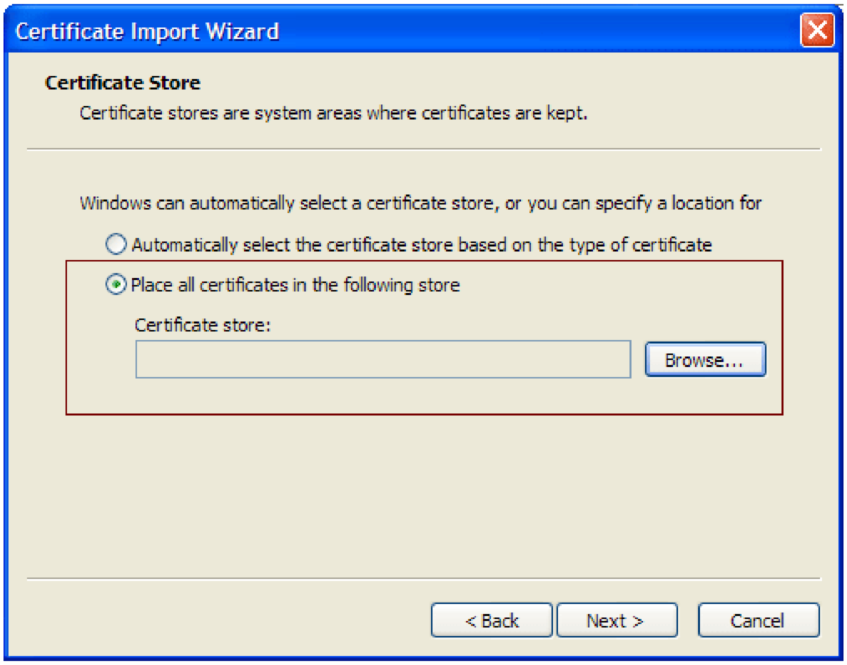
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

3. Select “Place all certificates in the following store,” and click Browse.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

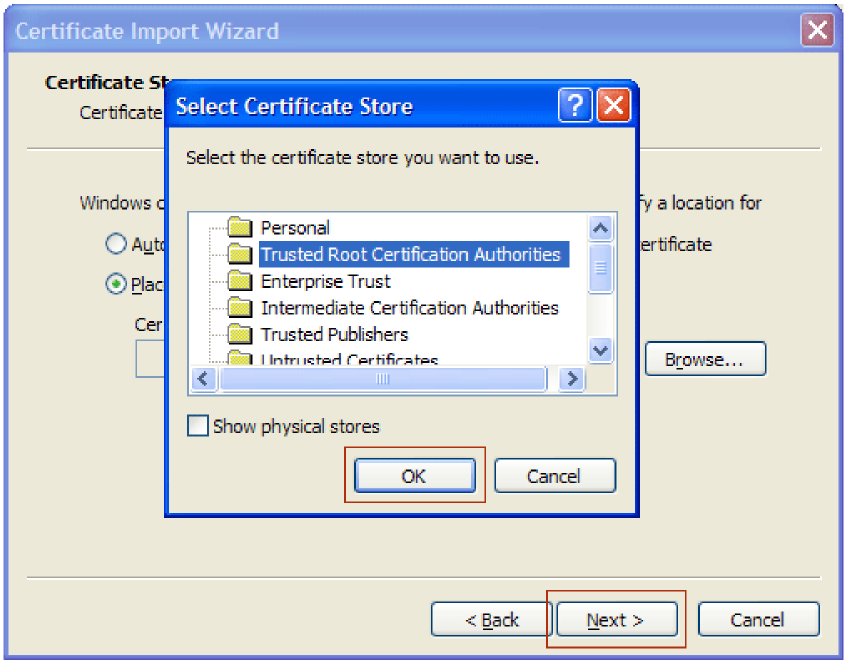
Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

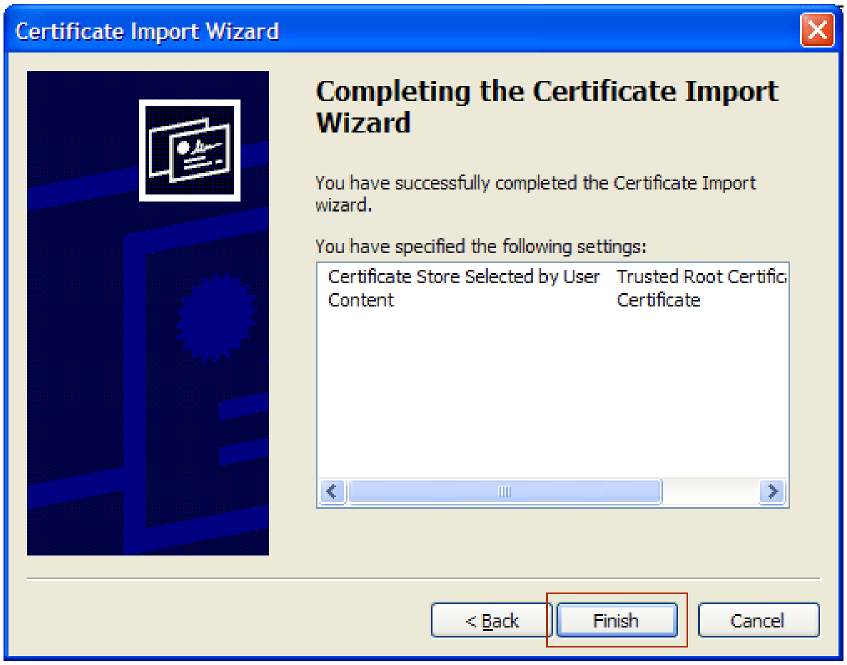
Certificate store:

4. Select the “Trusted Root Certification Authorities” directory, and click OK. Then, click the Next button.



Select the certificate store you want to use.

5. Click the Finish button.



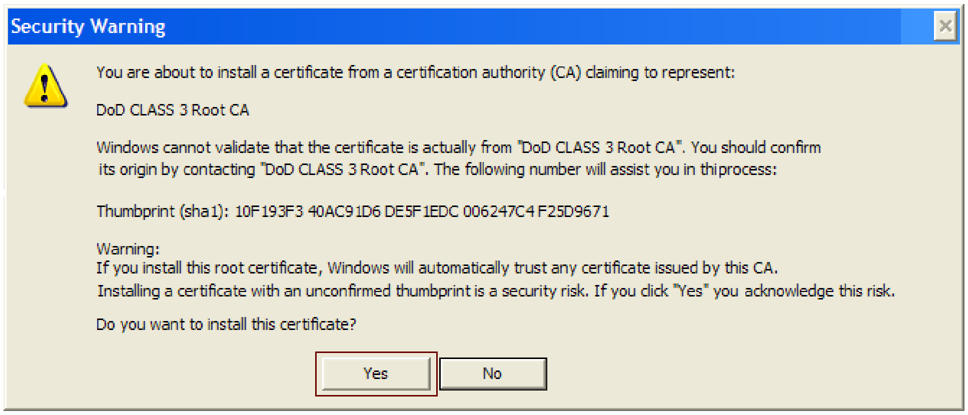
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate

You may receive a warning message that you are about to install a certificate that Windows cannot validate. This is normal. Click “Yes” to continue.



You are about to install a certificate from a certification authority (CA) claiming to represent:

DoD CLASS 3 Root CA

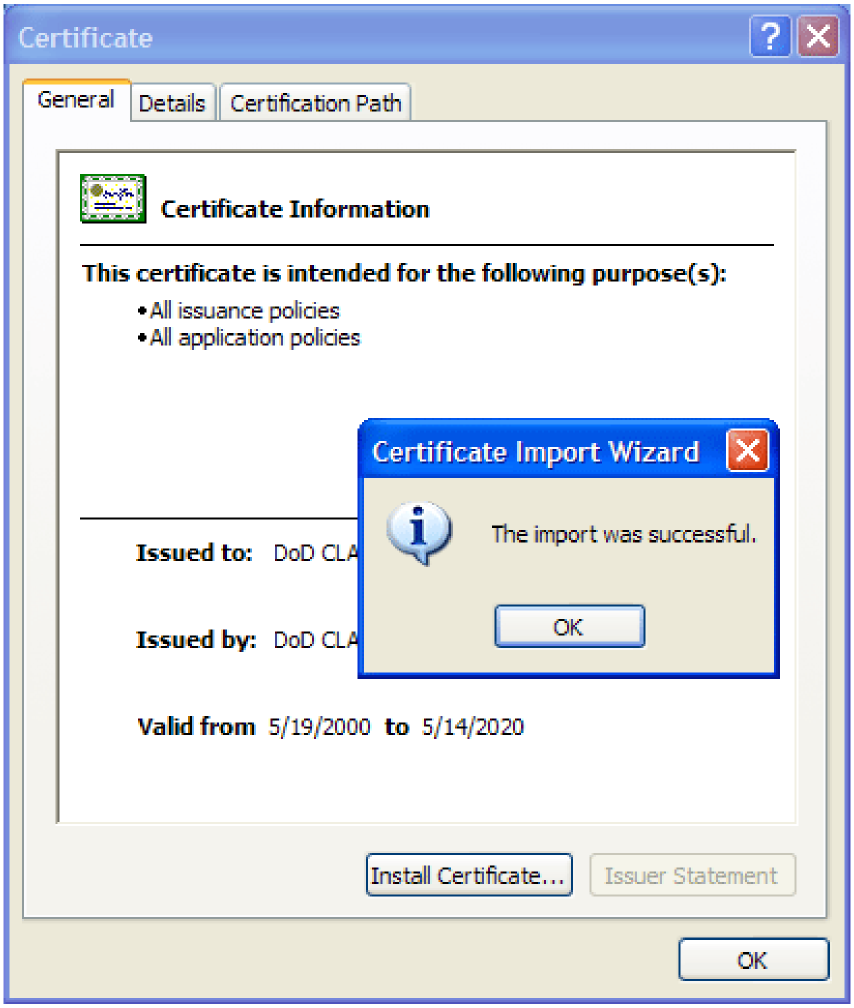
Windows cannot validate that the certificate is actually from "DoD CLASS 3 Root CA". You should confirm its origin by contacting "DoD CLASS 3 Root CA". The following number will assist you in thiprocess:

Thumbprint (sha1): 10F193F3 40AC91D6 DE5F1EDC 006247C4 F25D9671

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

You should receive a confirmation message, “The import was successful.”



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: DoD CLA

Issued by: DoD CLA

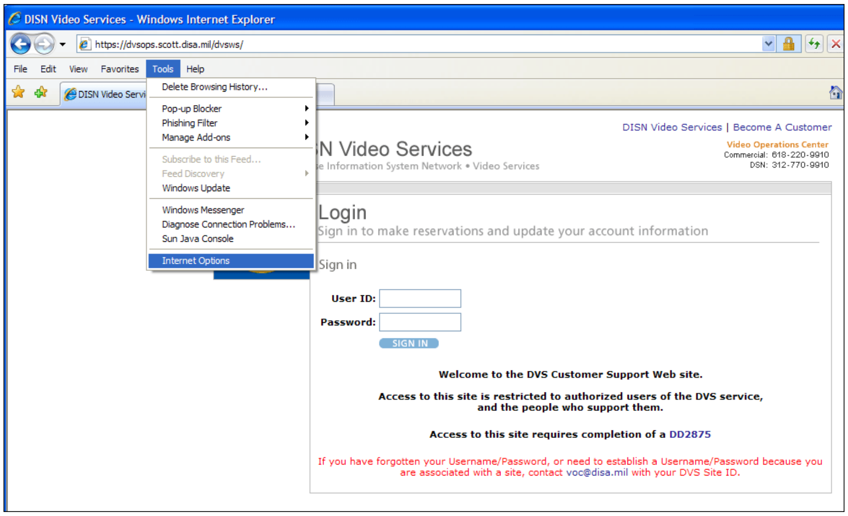
Valid from 5/19/2000 to 5/14/2020

The import was successful.

6. Repeat Steps 1 through 5 for the two other certificate files (i.e., "DoD Root CA 2.cer" and "ECA Root CA.cer"). Note that the certificates are available immediately. Restarting your computer or browser is not necessary.

5.1 Validating Certificate Installation in Internet Explorer

1. To validate the DoD Root Certificates have been installed in Microsoft Internet Explorer (IE), select Tools, then Internet Options.



DISN Video Services - Windows Internet Explorer
https://dvsops.scott.disa.mil/dvsws/
File
Edit
View
Favorites
Tools
Help
DISN Video Servi
Delete Browsing History...
Pop-up Blocker
Phishing Filter
Manage Add-ons
Subscribe to this Feed...
Feed Discovery
Windows Update
Windows Messenger
Diagnose Connection Problems...
Sun Java Console
Internet Options
DISN Video Services | Become A Customer
N Video Services
e Information System Network • Video Services
Login
Sign in
User ID:
Password:
SIGN IN

Video Operations Center
Commercial: 618-220-9910
DSN: 312-770-9910

Sign in to make reservations and update your account information

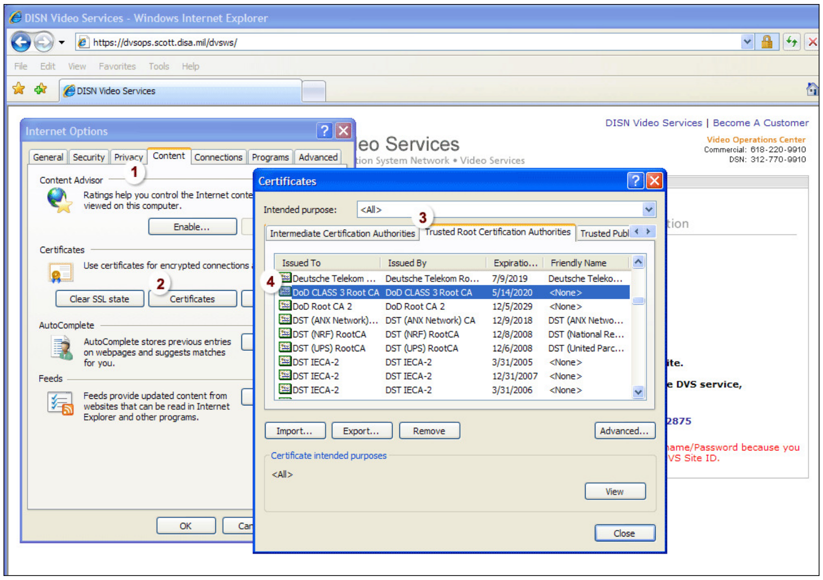
Welcome to the DVS Customer Support Web site.

Access to this site is restricted to authorized users of the DVS service, and the people who support them.

Access to this site requires completion of a DD2875

If you have forgotten your Username/Password, or need to establish a Username/Password because you are associated with a site, contact voc@disa.mil with your DVS Site ID.

2. Select the Content tab, click the Certificates button, and select the Trusted Root Certification Authorities tab. Then, scroll to find the DoD Root CA's.



Ratings help you control the Internet conte viewed on this computer.

Use certificates for encrypted connections a

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

Video Operations Center
Commercial: 618-220-9910
DSN: 312-770-9910

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Deutsche Telekom ...	Deutsche Telekom Ro...	7/9/2019	Deutsche Teleko...
DoD CLASS 3 Root CA	DoD CLASS 3 Root CA	5/14/2020	<None>
DoD Root CA 2	DoD Root CA 2	12/5/2029	<None>
DST (ANX Network)...	DST (ANX Network) CA	12/9/2018	DST (ANX Netwo...
DST (NRF) RootCA	DST (NRF) RootCA	12/8/2008	DST (National Re...
DST (UPS) RootCA	DST (UPS) RootCA	12/6/2008	DST (United Parc...
DST IECA-2	DST IECA-2	3/31/2005	<None>
DST IECA-2	DST IECA-2	12/31/2007	<None>
DST IECA-2	DST IECA-2	3/31/2006	<None>

Certificate intended purposes
<All>

ite.

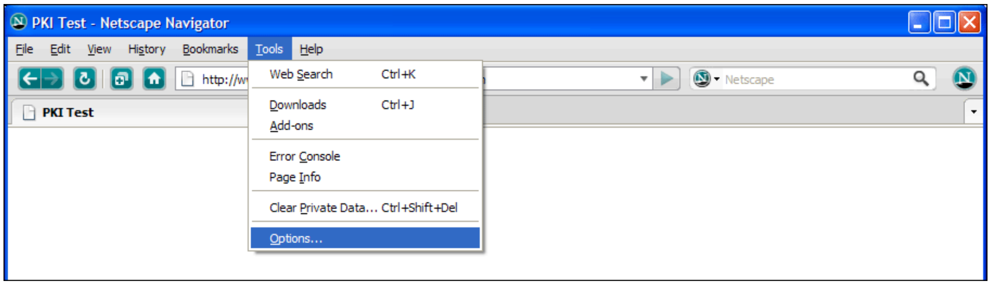
e DVS service,

2875

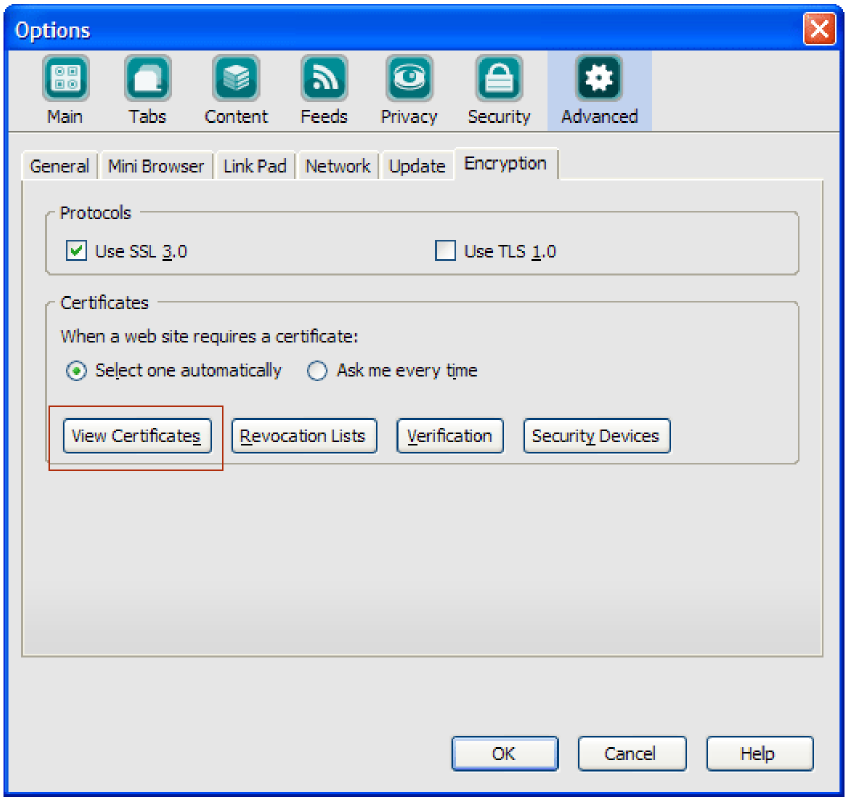
ame/Password because you
VS Site ID.

6.0 Install DoD Root CA Certificates in Netscape Navigator (v9.0)

1. Open Netscape. From the top menu select Tools, then Options. Note that installing the certificates is done through Netscape (not Windows).


PKI Test - Netscape Navigator
File Edit View History Bookmarks Tools Help
http://w
Netscape
PKI Test
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Error Console
Page Info
Clear Private Data... Ctrl+Shift+Del
Options...

2. From the Options windows select the Advanced tab, and click View Certificates.



Protocols

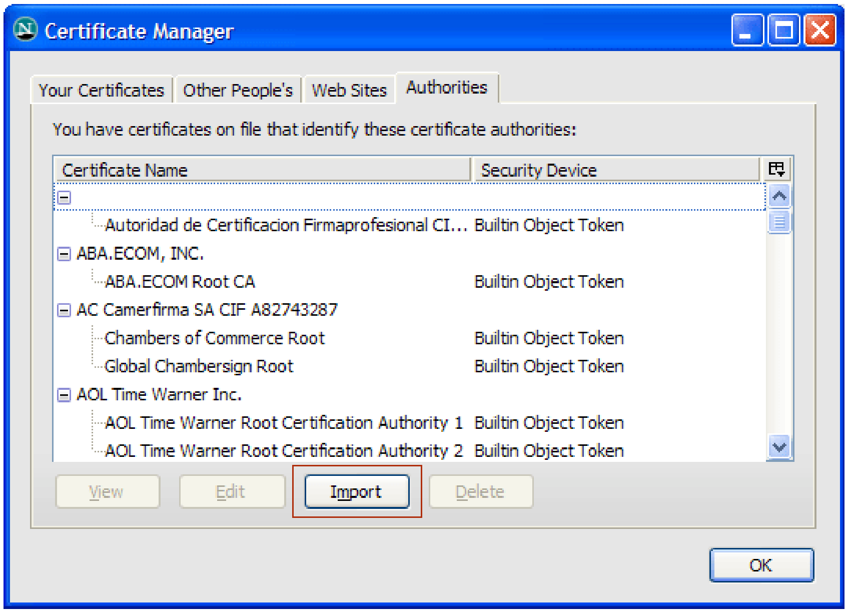
☑ Use SSL 3.0 ☐ Use TLS 1.0

Certificates

When a web site requires a certificate:

● Select one automatically ○ Ask me every time

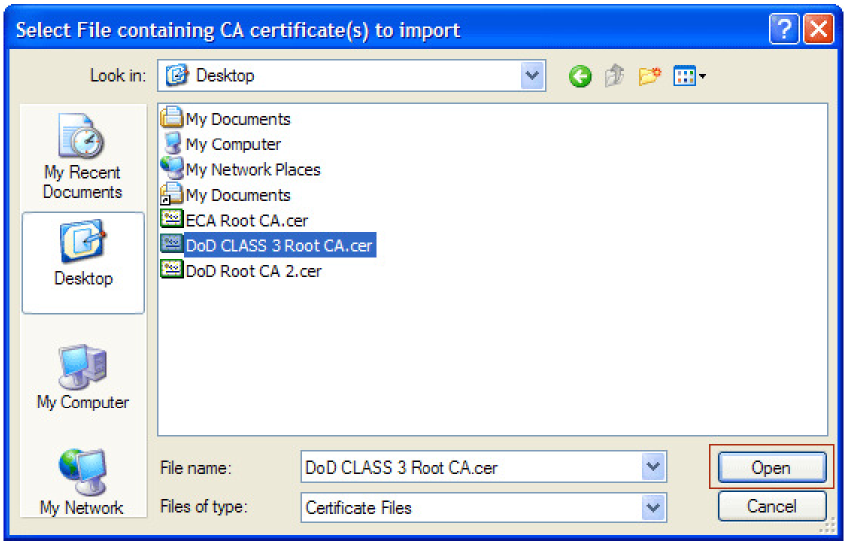
3. Select the Authorities tab, and click Import.



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
⊟	
Autoridad de Certificacion Firmaprofesional CI…	Builtin Object Token
⊟ ABA.ECOM, INC.	
ABA.ECOM Root CA	Builtin Object Token
⊟ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
⊟ AOL Time Warner Inc.	
AOL Time Warner Root Certification Authority 1	Builtin Object Token
AOL Time Warner Root Certification Authority 2	Builtin Object Token

4. Navigate to the location where you saved the certificate files (see Section 4.0 Download DoD Root Certificate Authority (CA) Certificates). Select the "DoD CLASS 3 Root CA.cer" file, and click Open.



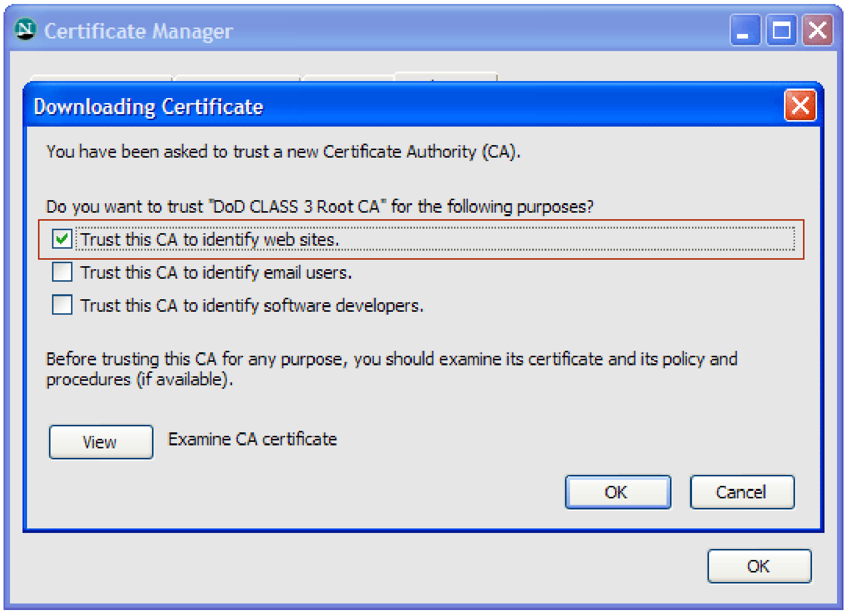
Look in: Desktop

My Documents
My Computer
My Network Places
My Documents
ECA Root CA.cer
DoD CLASS 3 Root CA.cer
DoD Root CA 2.cer

File name: DoD CLASS 3 Root CA.cer

Files of type: Certificate Files

5. In the Downloading Certificate window, check the "Trust this CA to identify web sites." box, and click OK.



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "DoD CLASS 3 Root CA" for the following purposes?

☑ Trust this CA to identify web sites.

☐ Trust this CA to identify email users.

☐ Trust this CA to identify software developers.

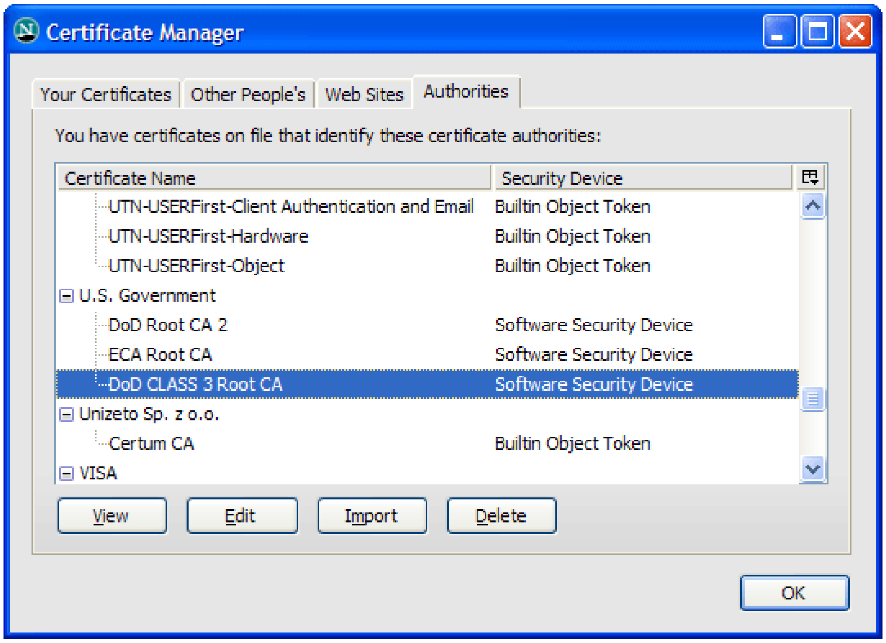
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

7. Repeat Steps 1 through 5 for the two other certificate files, i.e., "DoD Root CA 2.cer" and "ECA Root CA.cer". Note that the certificates are available immediately. Rebooting your computer or browser is not necessary.

6.1 Validating Certificate Installation in Netscape Navigator

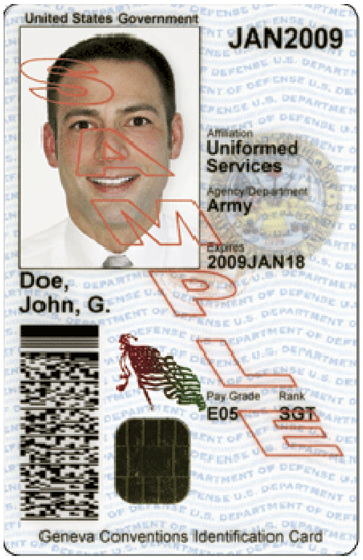
To validate the DoD Root Certificates have been installed in Netscape Navigator, select Tools, Options, Advanced tab, View Certificates, Authorities tab. Scroll the list to the section that says, "U.S. Government." Each certificate should be listed.



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
UTN-USERFirst-Client Authentication and Email	Builtin Object Token
UTN-USERFirst-Hardware	Builtin Object Token
UTN-USERFirst-Object	Builtin Object Token
⊟ U.S. Government	
DoD Root CA 2	Software Security Device
ECA Root CA	Software Security Device
DoD CLASS 3 Root CA	Software Security Device
⊟ Unizeto Sp. z o.o.	
Certum CA	Builtin Object Token
⊟ VISA	

7.0 PKI Smart Card Technology



A smart card resembles a credit card in size and shape, but inside it is completely different. First of all, it has an inside -- a normal credit card is a simple piece of plastic. The inside of a smart card usually contains an embedded microprocessor. The microprocessor is under a gold contact pad on one side of the card. The microprocessor on the smart card is there for security. The host computer and card reader actually "talk" to the microprocessor. The microprocessor enforces access to the data on the card.

7.1 Common Access Card (CAC)

The Common Access Card (CAC) is a DoD smartcard issued as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel. As of 6:30 PM EST, 28 February 2008, to login to DVS-WS you will be required to use a smart card reader and your DoD CAC card.

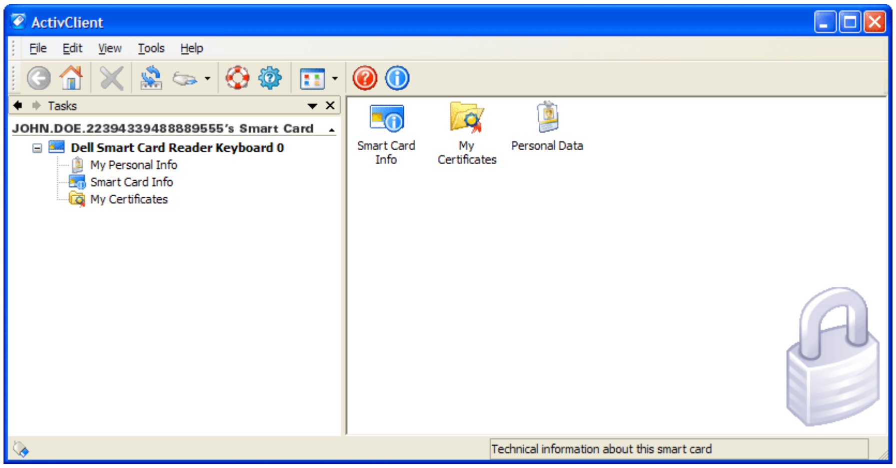
7.2 ECA Cards

DVS customers without a CAC card may use either an ECA (External Certificate Authority) or HSPD-12 card. ECA certificates provide secure identity verification for employees of companies, foreign governments, and individuals conducting business with DoD.

7.3 Using a CAC Card to Login to DVS-WS

These instructions assume the user has registered their certificate through the ActivClient and the certificate is recognized by the user's web browser (e.g., Internet Explorer (IE) or Netscape); if this is not the case, please contact the DISANet Help Desk at HelpDesk.DISANet@disa.mil or (703) 607-6600, DSN 327.

To test if ActivClient (and your smart card reader) is working correctly, open ActivClient and insert your CAC card. You should verify that ActivClient has found your Smart Card Info, My Certificates, and Personal Data. If this is not case, you will not be able to login to DVS-WS. Any problems at this stage must be resolved locally.



JOHN.DOE.22394339488889555's Smart Card

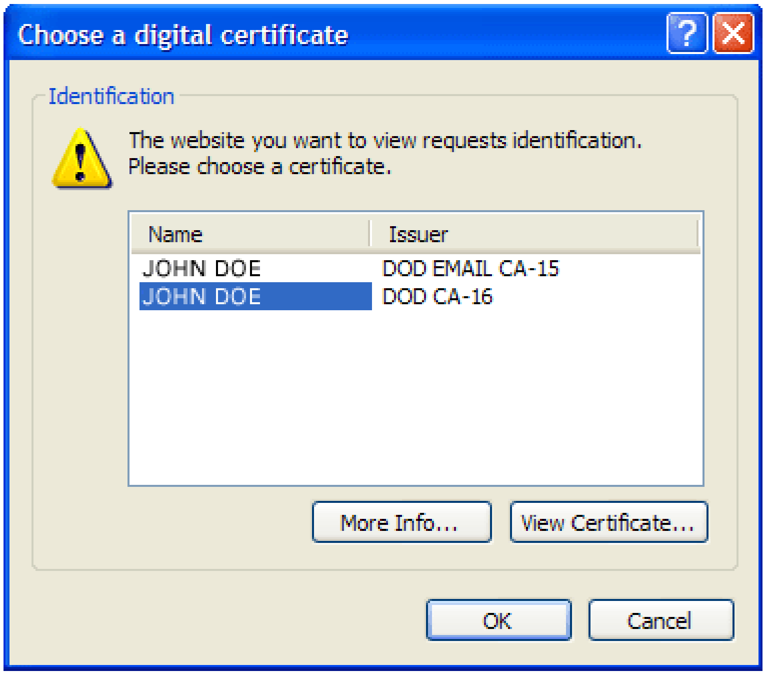
- Dell Smart Card Reader Keyboard 0
  - My Personal Info
  - Smart Card Info
  - My Certificates

Technical information about this smart card

If your CAC is working correctly, accessing DVS-WS is simply a matter of opening the URL in your browser: https://dvsops.scott.disa.mil.

IMPORTANT: You must use the DVS-WS domain name (https://dvsops.scott.disa.mil). If you use the IP address (https://209.22.91.136), you will receive a certificate-warning message even if the DoD Root certificates are installed properly. See Section 3.0 *Installing DoD Root Certificates* for more information.

You may be prompted to select a PKI certification located on your CAC card. In this example, we are selecting the DOD CA-16 certificate (not the email certificate). Then, press OK.



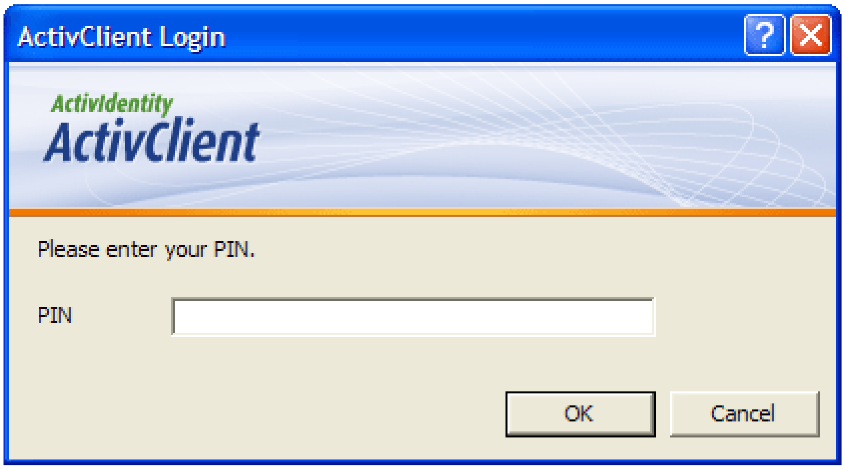
Choose a digital certificate

Identification

The website you want to view requests identification.
Please choose a certificate.

Name	Issuer
JOHN DOE	DOD EMAIL CA-15
JOHN DOE	DOD CA-16

You may also be prompted to enter your 6-digit (or 7-digit) PIN number that is encrypted on your CAC card. **Warning: Only three attempts are allowed before your card is locked.**

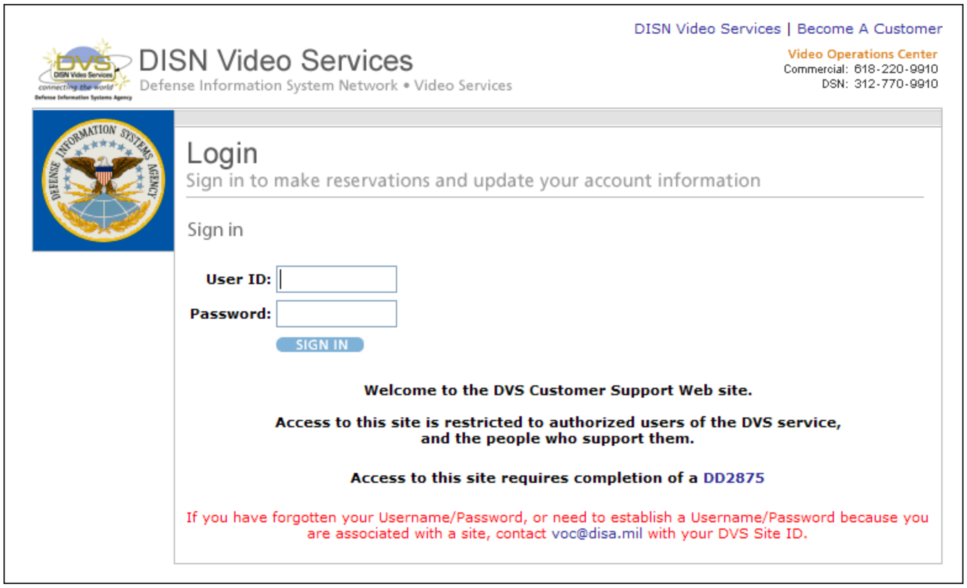


ActivClient Login

Please enter your PIN.

PIN

At this point you see the normal DVS-WS login screen. DVS Users will still use their current User ID and Password to access the DVS-WS application.



DISN Video Services | Become A Customer

DVS
DISN Video Services
connecting the world
Defense Information Systems Agency

DISN Video Services
Defense Information System Network • Video Services

Video Operations Center
Commercial: 618-220-9910
DSN: 312-770-9910

DEFENSE INFORMATION SYSTEMS AGENCY

Login
Sign in to make reservations and update your account information

Sign in

User ID:
Password:

Welcome to the DVS Customer Support Web site.

Access to this site is restricted to authorized users of the DVS service, and the people who support them.

Access to this site requires completion of a DD2875

If you have forgotten your Username/Password, or need to establish a Username/Password because you are associated with a site, contact voc@disa.mil with your DVS Site ID.

Figure 3. DVS-WS Login Screen

8.0 Frequently Asked Questions

8.1 What is Public Key Infrastructure?

A Public Key Infrastructure (PKI) (see http://iase.disa.mil/pki/) is the framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components of a PKI include system components such as one or more Certification Authorities and a certificate repository; documentation including a Certificate Policy document and one or more Certification Practice Statements; and trained personnel performing trusted roles to operate and maintain the system.

PKI integrates digital certificates, public-key cryptography, and Certification Authorities into total, enterprise-wide network security architecture. A typical enterprise PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

DoD Instruction 8520.2, “Public Key Infrastructure and Public Key Enabling” establishes the requirements for PK-enabling all activities (i.e., e-mail, private web servers, and networks).

8.2 What is Public Key-Enabling?

Public Key-enabling (PK-Enabling) is the process of configuring systems and applications to use certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation. PK-enabling of the DVS Web server(s) provides us with the capability to rely on digital certificates, in lieu of existing technologies such as usernames and passwords.

Certificate-based authentication consists of three steps: establishing an encrypted communication channel, validating the subscriber’s certificate, and performing a challenge-response between the DVS Web server and the DVS client to ensure that the user is the subscriber named in the certificate. If these three steps are successful, the DVS Web server can trust that the identity of the user is the same as the identity stated in the certificate and can then map that identity to authorizations.

8.3 What is DoD PKI?

DoD PKI is a fundamental component of the DoD’s Net-Centric vision and is essential to providing enhanced Information Assurance and Identity Management capabilities. It provides the base level of identification and authentication, integrity, non-repudiation and confidentiality for the Global Information grid. The DoD use of PKI in our Identity Management capability is recognized as the world leader in this area.

The DoD PKI is operated under the requirements of the DoD X.509 Certificate Policy. The Root Certification Authority (CA) is operated by NSA in an off-line state. This Root CA issues certificates to on-line Subordinate CAs on both the NIPRNet and the SIPRNet. Subordinate CAs issue certificates to subscribers, including both human and non-human entities such as web servers who have been authenticated by trusted individuals including Registration Authorities, Local Registration Authorities, and Verification Officers.

The DoD PKI issues certificates to both software and hardware tokens. The primary token for individuals within the DoD on the NIPRNet is the Common Access Card.

8.4 What is a CAC and how does it relate to software certificates and PKI?

The Common Access Card (CAC) is a Department of Defense (DoD) smart card (credit card-size device that contains one or more integrated circuits) initiative currently underway across the Agency. The CAC will serve as the following: standard ID card for active-duty military personnel (to include the Selected Reserve), DoD civilian employees, and eligible contractor personnel; principal card used to enable physical access to buildings and controlled spaces; principal card used to enable computer network and system access; and primary platform for the PKI authentication token. A CAC will contain a user’s software certificate, which is a computer-generated record that ties the user’s identification with the user’s public key in a trusted bond. The certificate contains the following (at a minimum): identity of the issuing Certification Authority, identity of the user, and the user’s public key. A Public Key Infrastructure (PKI) provides an electronic framework (i.e., software and a set of rules and practices) for secure communication and transactions between organizations and individuals. A PKI is based on asymmetric encryption and digital signatures technologies. For further information on DISA CAC and PKI initiatives, please view the DISA CAC (https://workspaces.disa.mil) web site.

8.5 Who may obtain a DoD PKI certificate?

DoD eligible users are active duty uniformed services personnel, members of the Selected Reserve, DoD civilian employees, and personnel working on site at DoD facilities using DoD network and e-mail services.

For personnel who are not DoD military or civilian employees, eligibility is determined based on the interaction of the individual with the DoD rather than on the type of individual. These personnel include DoD support contractors, non-US nationals, and volunteers. Individuals who access DoD information systems from a remote location, such as accessing web servers, are not generally eligible for DoD PKI certificates. Individuals who have a duty station within a DoD facility and who require direct access to DoD networks are generally eligible for DoD PKI certificates.

8.6 Who Is Not Eligible for a DoD PKI Certificate?

DoD eligible users are active duty uniformed services personnel, members of the Selected Reserve, DoD civilian employees, and personnel working on site at DoD facilities using DoD network and e-mail services. Individuals who access DoD information systems from a remote location, such as accessing web servers, are not generally eligible for DoD PKI certificates. Individuals who conduct business with, access DoD information systems over the Internet, or exchange e-mail with DoD entities are not eligible for DoD PKI certificates unless they also work on site at DoD facilities. DoD allies and coalition partners are not eligible for DoD PKI certificates unless they work on site at DoD facilities.

8.7 What is a DD Form 2875?

In compliance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and in meeting Information Assurance (IA) requirements, DD Form 2875, System Authorization Access Request (SAAR), is required of all DVS subscribers. All individuals MUST submit a DD Form 2875. However, obtaining a DVS User ID and Password is a completely separate process from obtaining a CAC card or ECA Certificate.

DD Form 2875, instructions to assist you in completing and faxing the form, and Frequently Asked Questions are available for downloading at http://www.disa.mil/disnvtc/become.htm.

8.8 What is a DoD PKI External Certification Authorities (ECA)?

The External Certification Authority (ECA) program is designed to provide a mechanism for external entities and organizations to get certificates that have been approved by the DoD as meeting the required DoD assurance level for binding the identity of the named certificate holder to the public key contained in the certificate. The ECA program is not restricted for use only by DoD applications. For more information about the ECA program, see http://iase.disa.mil/pki/eca.

8.9 Where can I obtain a CAC?

Please view the DISA CAC (https://workspaces.disa.mil) web site for further information. See also the "Common Access Card (CAC) User Guide" https://edge.disa.mil/DISA_CAC_Registration.pdf.

8.10 What are the steps to obtain an ECA certificate or card?

To obtain an ECA card requires:

- Enrollment with one of the 3 ECA issuers (see below)
- Request ECA online
- Provide verified required identification
- Pay fee (about $125 per individual per year)
- Receive ECA digital certificate
- Install ECA on PC, secure backup of ECA certificate
- Registration process specific to browser (IE or Netscape)
- ECA registry will promulgate registration to DoD Certificate Authority and Revocation List.

8.11 Where can I obtain an ECA Certificate?

ECA Certificates are obtained directly from the vendors. You may purchase an ECA Certificate from one of the following approved vendors:

- Operational Research Consultants: http://www.eca.orc.com/index.html
- VeriSign:http://www.verisign.com/verisign-business-solutions/public-sector-solutions/eca-certificates/index.html
- IdenTrust, Inc. (formerly DST) http://www.identrust.com/certificates/eca/index.html

Note: See each vendor's web site for pricing, system specifications, and instructions for obtaining, maintaining, and revoking your ECA certificate.

For more on how to obtain ECA certificates, see http://iase.disa.mil/pki/eca/certificate.html. For answers to frequently asked questions (FAQs) about the ECA PKI Program, and its offerings, see http://iase.disa.mil/pki/eca/frequently_asked_questions.html.

9.0 Trouble Shooting

9.1 My certificate is expired. How do I receive a new one?

Each certificate has a validity period after which it expires. This period is set when the certificate is written to your CAC. Please view the DISA CAC (https://workspaces.disa.mil) web site for further information.

9.2 My certificate is revoked. How do I receive a new one?

Your card may have been reported lost, stolen, or compromised. Please view the DISA CAC (https://workspaces.disa.mil) web site for further information.

9.3 How do I register a CAC?

Using IE, access the CAC registration page (https://intranet.disa.mil/pkiregistration/) and select "Register" under "CAC Registration". Read the instructions and information contained in the "CAC Registration Information" window and click "Register Certificate." Enter the user's e-mail address and DISA ID in the "CAC Registration Entry" window and select "Submit." An email message will be sent to the user containing a unique PKI Security Code. Enter this Code in the "CAC Registration - Enter Security Code" window and click "Submit." Select the user's certificate and enter the CAC PIN. Upon successful registration, the "CAC Registration Completion" window will display. Click "Finish" to close the browser window.

9.4 I am presented with more than one certificate in the Client Authentication window; which one do I select?

Some users may find more than one certificate available for selection. This scenario may occur if a user's CAC has recently expired, and the user was issued an updated certificate. The expired certificate will remain stored in the browser's list of available certificates, and therefore, display in the Client Authentication window. To determine the validity of each certificate, highlight one of the certificates from the list displayed in the Client Authentication window (click on the certificate name) and click "View Certificate." The details of the certificate will include the expiration date. To remove a certificate from displaying in the Client Authentication window, go to Tools --> Internet Options --> Content --> Certificates, select the appropriate certificate, and click “Remove.” [If the incorrect certificate was inadvertently deleted, it will automatically re-install once the CAC is placed in the reader.]

9.5 My certificate does not show up in the Client Authentication window, what do I do?

This may be due to one of the following reasons: your certificate is not installed/registered through ActivClient (DISA certificate management application); or, your certificate has never been used with the web browser before; or, your certificate is un-trusted by the DISA Intranet Web Server; or, your browser or CAC reader is configured incorrectly. If your certificate was not installed on this machine, please contact the DISANet Help Desk at HelpDesk.DISANet@disa.mil, or (703) 607-6600, DSN 327.

If your certificate has not been used by a web browser on this machine, enter your CAC into the reader to import your software certificate into the browser. If your certificate is un-trusted by the DISA Intranet Web Server, contact DISA Intranet Support for further assistance (Support@disa.mil or (703) 681-2327, DSN 761).

If you are attempting to register a software certificate, your certificate must be imported into the browser. To enter a software certificate within IE, go to Tools --> Internet Options --> Content --> Certificates --> Import and follow the wizard to find and import your certificate. To enter a software certificate within Netscape (7.0 or later), go to Edit --> Preferences --> Privacy & Security --> Certificates --> Manage Certificates --> Import and follow the instructions to import your certificate. To download the Root CA Certificate into Netscape, visit the DoD Class 3 PKI website and follow the provided instructions: http://dodpki.c3pki.chamb.disa.mil/rootca.html.

9.6 The Client Authentication window does not appear after clicking “Register Certificate.” How do I resolve this?

You may need to close the active browser window(s) and open a new one to attempt the process again. This scenario will occur when a user has cancelled out of a portion of the registration process. The browser will store a previous selection in its cache, which will require the user to clear the cache before making a different selection.

9.7 I was redirected to a “Page cannot be displayed” URL. What could be the cause?

There are two known circumstances when this will apply: the user has attempted to login or register an expired certificate, or the user has canceled out of the PIN entry window for their CAC. To rectify this problem, close the existing browser window and open a new window; this will clear the cache and enable the user to continue.

9.8 How do I verify the expiration date of my certificates?

To verify the expiration on your certificate using IE, select your certificate from the Client Authentication window, highlight the correct certificate, and click “View Certificate.” The certificate validity dates will be displayed at the bottom of the “General” tab. Your CAC also displays the expiration date in the bottom right corner on the face of the card. If you determine your card is valid, but are having trouble accessing DISA intranet applications, please contact DISA Intranet Support at Support@disa.mil or (703) 681-2327, DSN 761; or view the DISA CAC website for further information.

9.9 After placing my CAC in the reader, I get the following message: You have three (3) attempts to correctly enter your Personal Identification Number for your CAC. Why am I receiving this message?

After the third consecutive attempt, your CAC is locked and you will not have access to your PKI certificates. You may have your CAC unlocked at a CAC PIN Reset (CPR) workstation. Please view the DISA CAC website for further information.

10.0 PKI Policy and Guidance

Common Access Card Memorandum, November 10, 1999
Subject: "Smart Card Adoption and Implementation," the Department is implementing smart card technology through a common access card (CAC) and has developed four versions as described within this memorandum.
Link: https://www.cac.mil/assets/pdfs/DEPSECDEF_Policy.pdf

DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004
Subject: This Instruction implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a Department-wide Public Key Infrastructure (PKI) and enhancing the security of Department of Defense (DoD) information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. It aligns DoD PKI and PK (Public Key)-Enabling activities with DoD Directive 8500.1, as implemented by DoD Instruction 8500.2, and the DoD Common Access Card (CAC) program, as specified by DoD Directive 8190.3
Link: http://www.dtic.mil/whs/directives/corres/html/852002.htm

FIPS Publication 201-1, March 2006
Subject: Personal Identity Verification (PIV) of Federal Employees and Contractors
Link: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

Homeland Security Presidential Directive - 12 (HSPD-12), August 27, 2004
Subject: Policy for a Common Identification Standard for Federal Employees and Contractors
Link: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

11.0 Web Sites of Interest

DOD Access Card Office Homepage (for use by DoD personnel only)
Link: https://www.dmdc.osd.mil/swg/owa/WebGuard.Login?APPL=9010&RULE=08

DoD IA Strategic Plan Version 1.1, January 2004
Link: http://www.defenselink.mil/cio-nii/docs/DoD_IA_Strategic_Plan.pdf

FIPS Publications
Link: http://csrc.nist.gov/publications/PubsFIPS.html

Mission: Possible, Security to the Edge, August 2005
Link: http://iase.disa.mil/policy-guidance/IA_Glossy.pdf

NIST Computer Security Division, Computer Security Resource Center
Link: http://csrc.nist.gov/

Public Key Infrastructure (PKI)
Link: http://iase.disa.mil/pki/

Rapids Site Locator
Link: http://www.dmdc.osd.mil/rsl/owa/home

12.0 Appendix A: Acronyms

CA	Certificate Authority
CAC	Common Access Card
DISN	Defense Information System Network
DISA	Defense Information Systems Agency
DoD	Department of Defense
DST	Digital Signature Trust
DVS-WS	DISN Video Services - Web Site
ECA	External Certification Authority
IE	Microsoft Internet Explorer
PKE	Public Key Enablement
PKI	Public Key Infrastructure
PSM	Personal Security Manager
SP	Service Pack